Daniel Wichs

Contact Information

Office 340 West Village H
Northeastern Unviersity
440 Huntington Avenue
Boston, MA 02115

Phone: (650) 799-0567
E-mail: wichs@ccs.neu.edu
WWW: http://ccs.neu.edu/home/wichs

Citizenship United States

Research Interests

I am interested in all aspects of modern *cryptography* and more broadly *theoretical computer science* and *computer and network security.*

I am especially interested in:
- Homomorphic computation on cryptographic data
- Cryptography with weak sources of randomness
- Resilience to side-channel leakage and tampering attacks
- Lattice based cryptography
- Foundations of cryptography

Current Position

Northeastern University, Boston, MA — *Jan 2013 - present*
Assistant Professor of Computer Science

Education

New York University, New York, NY — *Sept 2006 - Sept 2011*
Ph.D. in Computer Science. *Sept, 2011.*
Research Advisor: Yevgeniy Dodis
Thesis: *Cryptographic Resilience to Continual Information Leakage*

Stanford University, Stanford, CA — *Sept 2001 - June 2005*
M.S. in Computer Science, *June, 2005.*
B.S. in Mathematics, *June, 2005.*

PostDoc

IBM Research, T.J. Watson Center, Yorktown Heights, NY — *Aug 2011 - Jan 2013*
Postdoctoral fellow supported by the *Josef Raviv Memorial Fellowship.*

Honors & Awards

- IBM Josef Raviv Memorial Postdoctoral Fellowship, 2011 - 2012.
- NYU Janet Fabri Prize , 2011: "Outstanding Dissertation in Computer Science".
- NYU Departmental Nominee for ACM Doctoral Dissertation Award, 2011.
- IBM Ph.D. Fellowship, 2010 - 2011.
- Courant Institute, Harold Grad Memorial Prize 2010.
- Invited Talks at Major Conferences and Workshops
  - *Non-Malleable Codes*
    Invited keynote at the IMA International Conference on Cryptography and Coding (IMACC) 2015.
  - *Tamper-Detection and Non-Malleable Codes*
    Invited talk at the International Conference on Information-Theoretic Security (ICITS) 2015.
- Papers invited to special issues of journals
  - *Essentially Optimal Robust Secret Sharing with Maximal Corruptions*
    Honorable mention for best paper award at EUROCRYPT 2016 (top 3 papers).
    Invited to Journal of Cryptology.

- *On the Implausibility of Differing-Inputs Obfuscation.*
  Invited to Algorithmica special issue on selected papers from CRYPTO 2014.
- *How to Eat Your Entropy and Have it Too – Optimal Recovery Strategies for Compromised RNGs.*
  Invited to Algorithmica special issue on selected papers from CRYPTO 2014
- *Fully Leakage-Resilient Signatures*
  Invited to Journal of Cryptology special issue on selected papers from Eurocrypt 2011.
- *Efficient Public-Key Cryptography in the Presence of Key Leakage*
  Invited to Journal of Cryptology special issue on selected papers from Asiacrypt 2010.

Professional Activities

General Chair: STOC 2016

Program Committees:
Theory of Cryptography Conference (TCC) 2017
EUROCRYPT 2017.
Foundations of Computer Science (FOCS) 2016.
Theory of Cryptography Conference (TCC) 2015.
ASIACRYPT 2014.
Public-Key Cryptography (PKC) 2014.
Innovations in Theoretical Computer Science (ITCS) 2014.
CRYPTO 2013.
Theory of Cryptography Conference (TCC) 2012.
Security and Cryptography for Networks (SCN) 2012.
International Conference on Information Theoretic Security (ICITS) 2012.
International Conference on Information Theoretic Security (ICITS) 2011.

Boston Crypto Day (2014-current):
Co-organize Boston Area Crypto Day, a full day of talks on various topic in cryptography held twice per semester. Attended by a wide body of cryptography researchers from universities and research labs in the greater Boston area.

Northeastern Theory Reading Group (2014-current).
Co-organize the NEU theory reading group.

NYC CryptoDay (2011-2013):
Co-organized *New-York Area CryptoDay.*

Conference/Journal Refereeing:
I regularly review cryptography related articles for major conferences and journals such as: CRYPTO, EUROCRYPT, ASIACRYPT, TCC, PKC, FOCS, STOC, ICALP, CCS, Journal of Cryptology, SIAM Journal on Computing, Journal of the ACM, etc.

Thesis Committees:
Scott Roche, Northeastern University. Nov, 2016
Zahra Jafargholi (advisor), Northeastern. August, 2016
Vanishree Rao, UCLA. July, 2015.
Travis Mayberry, Northeastern University. July, 2015.
Benjamin Fuller, Boston University. November, 2014.
Eric Miles, Northeastern University. April, 2014.
Nico Dotling, Karlsruhe University, Germany. May, 2014.

PhD Students

- Zahra Jafargholi (graduated) *Sept 2013 - August 2016.*
  → *Postdoc at Aarhus University, Denmark.*

- Giorgos Zirdelis — *Sept 2015 - present.*
- Tanay Mehta — *Sept 2015 - present.*
- Ariel Hamlin — *Sept 2016 - present.*

Postdocs

- Alessandra Scafuro (joint with BU) — *Jan 2015 - August 2016.*
  → *Assistant Professor of Computer Science at North Carolina State.*
- Mor Weiss — *Sept 2016 - present.*

Visitors

- Alain Passelegue (PhD student, Ecole Normale Superieure PARIS) — *Sept 2015 - Jan 2016*
- Ryo Nishimaki (researcher, NTT laboratories) — *October 2014 - Jan 2016*
- Pratyay Mukherjee (PhD student, Aarhus University) — *June 2014 - June 2015*
- Pavel Hubacek (PhD student, Aarhus University) — *Sept 2013 - Feb 2014*
- Yevgeniy Dodis (Prof., NYU) — *Jan - August 2013*

Funding

- NSF Frontier Trustworthy Computing Grant (# 1413964), 9/2014 - 8/2019,
  "MACS: A Modular Approach to Cloud Security".
  Amount to PI Wichs: **$800,000**.
- Google Faculty Research Award, 2103.
  "New Methods for Deriving Keys from Passwords" 2013.
  Amount to PI Wichs **$24,500**.
- NSF EAGER Grant (#1347350), 9/2013 - 1/2015.
  " Holistic Security for Cloud Computing: Oblivious Computation".
  Amount to PI Wichs: **$100,000** .
- NSF Medium Trustworthy Computing Grant (#1314722), 8/2013-7/2017.
  "The Theory and Practice of Key Derivation".
  Amount to PI Wichs: **$531,235**.

Publications

Google Scholar Statistics (as of 9/14/16): citations: 2,645, h-index: 27, i10-index: 42

[1] Zahra Jafargholi, Daniel Wichs
Adaptive Security of Yao's Garbled Circuits
TCC 2016

[2] Nir Bitansky, Ryo Nishimaki, Alain Passelgue, Daniel Wichs **From Cryptomania to Obfustopia through Secret-Key Functional Encryption**
TCC 2016

[3] Dennis Hofheinz, Vanishree Rao and Daniel Wichs
Standard Security Does Not Imply Indistinguishability Under Selective Opening
TCC 2016

[4] Yevgeniy Dodis, Shai Halevi, Ron Rothblum and Daniel Wichs
Spooky Encryption and its Applications
CRYPTO 2016

[5] Brett Hemenway, Zahra Jafargholi, Rafi Ostrovsky, Alessandra Scafuro and Daniel Wichs
Adaptively Secure Garbled Circuits from One-Way Functions
CRYPTO 2016

[6] Aloni Cohen, Justin Holmgren, Ryo Nishimaki , Vinod Vaikuntanathan and Daniel Wichs
Watermarking Cryptographic Capabilities
STOC 2016

[7] Allison Bishop, Valerio Pastro, Rajmohan Rajaraman and Daniel Wichs
Essentially Optimal Robust Secret Sharing with Maximal Corruptions
EUROCRYPT 2016

[8] Ryo Nishimaki, Daniel Wichs, and Mark Zhandry
Anonymous Traitor Tracing: How to Embed Arbitrary Information in a Key
EUROCRYPT 2016

[9] Pratyay Mukherjee and Daniel Wichs
Two Round Mutliparty Computation via Multi-Key FHE
EUROCRYPT 2016

[10] Zvika Brakerski, Vinod Vaikuntanathan, Hoeteck Wee and Daniel Wichs
Obfuscating Conjunctions under Entropic Ring LWE
TCC 2016

[11] Srini Devadas, Marten van Dijk, Chris Fletcher, Ling Ren, Elaine Shi and Daniel Wichs
Onion ORAM: A Constant Bandwidth Blowup Oblivious RAM
TCC 2016

[12] Perfect Structure on the Edge of Chaos
Nir Bitansky, Omer Paneth and Daniel Wichs
TCC 2016

[13] Tatsuaki Okamoto, Krzysztof Pietrzak, Brent Waters and Daniel Wichs
New Realizations of Somewhere Statistically Binding Hashing and Positional Accumulators
ASIACRYPT 2015

[14] Sergey Gorbunov, Vinod Vaikuntanathan and Daniel Wichs
Leveled Fully Homomorphic Signatures from Standard Lattices
STOC 2015 – Symposium on Theory of Computing.

[15] Vadim Lyubashevsky and Daniel Wichs
Simple Lattice Trapdoor Sampling from a Broad Class of Distributions
PKC 2015 – Public-Key Cryptography.

[16] Zahra Jafargholi and Daniel Wichs
Tamper Detection and Continuous Non-Malleable Codes
TCC 2015 – Theory of Cryptography Conference.

[17] Pavel Hubacek and Daniel Wichs
On the Communication Complexity of Secure Function Evaluation with Long Output
ITCS 2015 – Innovations in Theoretical Computer Science.

[18] Craig Gentry and Shai Halevi and Mariana Raykova and Daniel Wichs
Outsourcing Private RAM Computation
FOCS 2014 - Foundations of Computer Science.

[19] Sanjam Garg, Craig Gentry, Shai Halevi and Daniel Wichs
On the Implausibility of Differing-Inputs Obfuscation and Extractable Witness Encryption with Auxiliary Input
CRYPTO 2014 - Advances in Cryptology.

[20] Yevgeniy Dodis and Adi Shamir and Noah Stephens-Davidowitz and Daniel Wichs
How to Eat Your Entropy and Have it Too – Optimal Recovery Strategies for Compromised RNGs
CRYPTO 2014 - Advances in Cryptology.

[21] Craig Gentry, Shai Halevi, Steve Lu, Rafail Ostrovsky, Mariana Raykova and Daniel Wichs
Garbled RAM, Revisited
EUROCRYPT 2014 - Advances in Cryptology.

[22] Sebastian Faust, Pratyay Mukherjee, Daniele Venturi and Daniel Wichs
Efficient Non-Malleable Codes and Key-Derivation for Poly-Size Tampering Circuits
EUROCRYPT 2014 - Advances in Cryptology.

[23] Yevgeniy Dodis, Krzysztof Pietrzak and Daniel Wichs
Key Derivation without Entropy Waste
EUROCRYPT 2014 - Advances in Cryptology.

[24] Shweta Agrawal, Yevgeniy Dodis, Vinod Vaikuntanathan and Daniel Wichs
On Continual Leakage of Discrete Log Representations
ASIACRYPT 2013 – Advances in Cryptology.

[25] Rosario Gennaro and Daniel Wichs
Fully Homomorphic Message Authenticators
ASIACRYPT 2013 – Advances in Cryptology.

[26] Yevgeniy Dodis, David Pointcheval, Sylvain Ruhault, Damien Vergnaud and Daniel Wichs
Security Analysis of Pseudo-Random Number Generators with Input: /dev/random is not Robust
CCS 2013. – ACM Conference on Computer and Communications Security.

[27] Joel Alwen, Stephan Krenn, Krzysztof Pietrzak and Daniel Wichs
Learning with Rounding, Revisited: New Reduction, Properties and Applications
CRYPTO 2013. – Advances in Cryptology.

[28] Craig Gentry, Kenneth A. Goldman, Shai Halevi, Charanjit Jutla, Mariana Raykova and Daniel Wichs
Optimizing ORAM and Using it Efficiently for Secure Computation
PETS 2013. – Privacy Enhancing Technologies.

[29] Carmit Hazay, Adriana Lpez-Alt, Hoeteck Wee and Daniel Wichs
Leakage-Resilient Cryptography from Minimal Assumptions
EUROCRYPT 2013. – Advances in Cryptology.

[30] David Cash, Alptekin Kp and Daniel Wichs
Dynamic Proofs of Retrievability via Oblivious RAM
EUROCRYPT 2013. – Advances in Cryptology.

[31] Nir Bitansky, Dana Dachman-Soled, Sanjam Garg, Abhishek Jain, Yael Tauman Kalai, Adriana Lopez-Alt, Daniel Wichs.
Why "Fiat-Shamir for Proofs" Lacks a Proof.
TCC 2013 – Theory of Cryptography Conference.

[32] Daniel Wichs.
Barriers in Cryptography with Weak, Correlated and Leaky Sources.
ITCS 2013 – Innovations in Theoretical Computer Science.

[33] Gilad Asharov, Abhishek Jain, Adriana Lpez-Alt, Eran Tromer, Vinod Vaikuntanathan, Daniel Wichs.
Multiparty Computation with Low Communication, Computation and Interaction via Threshold FHE.
Eurocrypt 2012 – Advances in Cryptology.

[34] Yevgeniy Dodis, Eike Kiltz, Krzysztof Pietrzak, Daniel Wichs.
Message Authentication, Revisited
Eurocrypt 2012 – Advances in Cryptology.

[35] Yevgeniy Dodis, Abhishek Jain, Tal Moran, Daniel Wichs.
Counterexamples to Hardness Amplification Beyond Negligible.
TCC 2012 – Theory of Cryptography Conference.

[36] Yevgeniy Dodis, Allison Lewko, Brent Waters, Daniel Wichs
Storing Secrets on Continually Leaky Devices.
FOCS 2011 – Foundations of Computer Science.

[37] Stefan Dziembowski, Tomasz Kazana, Daniel Wichs
Key-Evolution Schemes Resilient to Space-Bounded Leakage.
CRYPTO 2011 – Advances in Cryptology.

[38] Craig Gentry and Daniel Wichs
Separating Succinct Non-Interactive Arguments From All Falsifiable Assumptions.
STOC 2011 – Symposium on Theory of Computing.

[39] Elette Boyle, Gil Segev, Daniel Wichs
Fully Leakage-Resilient Signatures.
EUROCRYPT 2011 – Advances in Cryptology.
Journal of Cryptology.

[40] Stefan Dziembowski, Tomasz Kazana, Daniel Wichs
One-Time Computable Self-Erasing Functions.
TCC 2011 – Theory of Cryptography Conference

[41] Yevgeniy Dodis, Kristiyan Haralambiev, Adriana Lopez-Alt, Daniel Wichs.
Efficient Public-Key Cryptography in the Presence of Key Leakage.
ASIACRYPT 2010 – Advances in Cryptology.
Invited to *Journal of Cryptology.*

[42] Yevgeniy Dodis, Kristiyan Haralambiev, Adriana Lopez-Alt, Daniel Wichs.
Cryptography Against Continuous Memory Attacks.
FOCS 2010 – Foundations of Computer Science.

[43] Joel Alwen, Yevgeniy Dodis, Moni Naor, Gil Segev, Shabsi Walfish, Daniel Wichs.
Public-Key Encryption in the Bounded-Retrieval Model.
EUROCRYPT 2010 – Advances in Cryptology.

[44] Ran Canetti, Yael Tauman Kalai, Mayank Varia, Daniel Wichs.
On Symmetric Encryption and Point Obfuscation.
TCC 2010 – Theory of Cryptography Conference.

[45] Stefan Dziembowski, Krzysztof Pietrzak, Daniel Wichs.
Non-malleable Codes.
ICS 2010 – Innovations in Computer Science.

[46] Juan Garay, Daniel Wichs, Hong-Sheng Zhou.
Somewhat Non-Committing Encryption and
Efficient Adaptively Secure Oblivious Transfer.
CRYPTO 2009 – Advances in Cryptology.

[47] Joel Alwen, Yevgeniy Dodis, Daniel Wichs.
Leakage-Resilient Public-Key Cryptography in the Bounded-Retrieval Model.
CRYPTO 2009 – Advances in Cryptology.

[48] Yevgeniy Dodis and Daniel Wichs.
Non-Malleable Extractors and Symmetric Key Cryptography from Weak Secrets.
STOC 2009 – Symposium on Theory of Computing.

[49] Yevgeniy Dodis, Salil Vadhan, Daniel Wichs.
Proofs of Retrievability via Hardness Amplification.
TCC 2009 – Theory of Cryptography Conference.

[50] Ivan Damgård, Jesper Buus Nielsen, Daniel Wichs.
Universally Composable Multiparty Computations with Partially Isolated Parties.
TCC 2009 – Theory of Cryptography Conference.

[51] Ivan Damgård, Jesper Buus Nielsen, Daniel Wichs.
Isolated Proofs of Knowledge and Isolated Zero Knowledge.
EUROCRYPT 2008 – Advances in Cryptology.

[52] Ronald Cramer, Yevgeniy Dodis, Serge Fehr, Carles Padró, Daniel Wichs.
Detection of Algebraic Manipulation with Applications to Robust Secret Sharing and Fuzzy Extractors.
EUROCRYPT 2008 – Advances in Cryptology.

Surveys

[1] Joel Alwen, Yevgeniy Dodis and Daniel Wichs.
Survey: Leakage Resilience and the Bounded Retrieval Model.
ICITS 2009 – International Conference on Information Theoretic Security.

Presentations & Invited Talks

Spookily Homomorphic Encryption
University of Michigan Theory Seminar. Ann Arbor, MIT. Nov, 2016.

Obfuscating Conjunctions under Entropic Ring LWE
Innovations in Theoretical Computer Science (ITCS). Cambridge, MA. January, 2016.

Homomorphic Cryptography beyond FHE
Departmental Seminar at UT Austin. Austin, TX. April, 2016.
NYC Theory Day. New York, NY. November, 2015.

Fully Homomorphic Commitments and Signatures
Simons Institute, Summer on Cryptography: Mathematics of Cryptography. Berkeley, CA. July, 2015.

Multi-Key Fully Homomorphic Encryption and Two-Round MPC
Bay Area Crypto Day. Stanford, CA. May, 2016.
Eurocrypt. Vienna, Austria. May, 2016.
Nexus of Information and Computation Theories at Institut Henri Pincare. Paris, France. March, 2016.
NYC Crypto Day at Cornell Tech. New York, NY. March, 2016.
Simons Institute, Summer on Cryptography: Securing Computation. Berkeley, CA. June, 2015.

Oblivious RAM with Server Computation
Simons Institute, Summer on Cryptography: Boot Camp. Berkeley, CA. May, 2015.

Tamper-Detection and Non-Malleable Codes
ICERM Algorithmic Coding Theory Workshop. Providence RI. June, 2016.
IMA International Conference on Cryptography and Coding (IMACC). December, 2015.
International Conference on Information-Theoretic Security (ICITS), Invited Talk. May, 2015.
Northeastern Mathematics Department Colloquium. April, 2015.
DIMACS Workshop on Coding-Theoretic Methods for Network Security. Rutgers, NJ. March, 2014.

On the Communication Complexity of Secure Function Evaluation with Long Output
MIT Cryptography and Information Security Seminar. Cambridge, MA. November, 2014.

On the Implausibility of Differing-Inputs Obfuscation
CRYPTO Conference. Santa Barbara, CA. August, 2014.

Optimal Recovery Strategies for Compromised RNGs
Ecole Normale Superieure (ENS), cryptography seminar. Paris, France. June, 2014.

Outsourcing Garbled RAM Computation
Oberwolfach Mathematical Institute - workshop in cryptography. Oberwolfach, Germany. July, 2014.
Ecole Normale Superieure (ENS), cryptography seminar. Paris, France. June, 2014.
Eurocrypt Conference (EUROCRYPT 2014). Copenhagen, Denmark. May, 2014.
Workshop on Theory and Practice of Multiparty Computation. Aarhus, Denmark. May, 2014
NYC CryptoDay. New York. April, 2014.
MIT Cryptography and Information Security Seminar. Cambridge, MA, USA. March, 2014.
A Workshop in Celebration of Goldwasser-Micali's Turing Award. Weizmann Institute, Israel. Dec 2013.

Dynamic Proofs of Retrievability via Oblivious RAM
DIMACS Workshop on "Current Trends in Cryptography". New York, NY, USA. May 2013.
IACR Eurocrypt Conference (EUROCRYPT 2013). Athens, Greece. May, 2013.

Barriers in Cryptography with Weak, Correlated and Leaky Sources
ITCS – Innovations in Theoretical Computer Science, Berkeley, CA. Jan, 2013.
Charles River Crypto Day at Boston University, Boston, MA, USA. November, 2012.

Counterexamples to Hardness Amplification Beyond Negligible.
Theory of Cryptography Conference, TCC 2012. Taormina, Italy. March 19, 2012.

Maintaining Security Under Imperfect Secrecy
Northeastern College of Computer and Information Science Colloquium. January 30, 2012.
IBM Research Colloquium. January 23, 2012.

Storing Secrets on Continually Leaky Devices.
52st IEEE Foundations of Computer Science (FOCS 2011). Palm Spring, CA, USA. October, 2011.
Faces of Modern Cryptography: A Day of Lectures. New York, NY, USA. September, 2011.

Separating Succinct Non-Interactive Arguments From All Falsifiable Assumptions.
Tel Aviv University Seminar. Tel Aviv, Israel. April, 2012.
43rd ACM Symposium on Theory of Computing (STOC 2011). San Jose, CA, USA. June, 2011.
Microsoft Research Seminar. Redmond, WA. June, 2011.
New York Area Crypto Day. New York, NY, USA. March, 2011.
Centrum Wiskunde & Informatica (CWI) Seminar. Amsterdam, Netherlands. January, 2011.
MIT Cryptography and Information Security Seminar. Cambridge, MA, USA. December, 2010.

Cryptography Against Continuous Memory Attacks.
51st IEEE Foundations of Computer Science (FOCS 2010). Las Vegas, NV, USA. October, 2010.
IBM Cryptography and Network Security Seminar, Hawthorne, NY, USA. October, 2010.
China Theory Week. Beijing, China. September, 2010.
Weizmann Institute Cryptography Seminar. Rehovot, Israel. May, 2010.
New York Area Crypto Day. New York, NY, USA. April, 2010.
MIT/Microsoft Joint Cryptography and Information Security Seminar. Cambridge, MA, USA. April, 2010.

Public-Key Encryption in the Bounded-Retrieval Model.
29th IACR Eurocrypt Conference (EUROCRYPT 2010). Nice, France. May, 2010.
Weizmann Institute Cryptography Seminar. Rehovot, Israel. May, 2010.
IBM Cryptography Seminar. Hawthorne, NY, USA. December, 2009.
NYU Cryptography Reading Group. New York, NY, USA. December, 2009.
MIT/Microsoft Joint Cryptography and Information Security Seminar. Cambridge, MA, USA. Nov, 2009.

On Symmetric Encryption and Point Obfuscation.
7th IACR Theory of Cryptography Conference (TCC 2010). Zurich, Switzerland. February, 2010.

Non-malleable Codes.
1st Innovations in Computer Science Conference (ICS 2010). Beijing, China. January, 2010.
Workshop on Provable Security against Physical Attacks. Leiden, Netherlands. February, 2010.
NYU Cryptgoraphy Reading Group. New York, NY, USA. March, 2010.

Leakage-Resilient Public-Key Cryptography in the Bounded-Retrieval Model.
29th IACR International Cryptology Conference (CRYPTO 2009). August, 2009.
NYU Cryptgoraphy Reading Group. New York, NY, USA. April, 2009.

Non-Malleable Extractors and Symmetric Key Cryptography from Weak Secrets.
41st ACM Symposium on Theory of Computing (STOC 2009). Bethesda, MD, USA. May, 2009.
Computer Science Colloquium at the University of Rome La Sapienza. Rome, Italy. February, 2009.
MIT/Microsoft Joint Cryptography and Information Security Seminar. Cambridge, MA, USA. Dec, 2009.

Proofs of Retrievability via Hardness Amplification.
6th IACR Theory of Cryptography Conference (TCC 2009). San Francisco, CA, USA. March 2009.

Universally Composable Multiparty Computation with Partially Isolated Parties.
6th IACR Theory of Cryptography Conference (TCC 2009). San Francisco, CA, USA. March 2009.

Isolated Proofs of Knowledge and Isolated Zero Knowledge.
27th IACR Eurocrypt Conference (EUROCRYPT 2008). Istanbul, Turkey. April, 2008.
MIT Cryptography and Information Security Seminar. Cambridge, MA, USA. April, 2008.
NYU Cryptography Reading Group. New York, NY, USA. November, 2007.

Detection of Algebraic Manipulation with Applications to Robust Secret Sharing and Fuzzy Extractors.
27th IACR Eurocrypt Conference (EUROCRYPT 2008). Istanbul, Turkey. April, 2008.
NYU Cryptography Reading Group. New York, NY, USA. September, 2008.

Research Positions

IBM – T.J. Watson Research Center. Hawthorne, NY. **Sept. 2011 - Jan. 2013**
Josef Raviv Memorial Postdoctoral Fellow

New York University – Courant Institute. New York, NY. **Sept. 2006 - Sept. 2011**
Research Assistant with Prof. Yevgeniy Dodis.

IBM – T.J. Watson Research Center. Hawthorne, NY. **Summer 2010**
Summer Research Intern with Dr. Tal Rabin

Weizmann Institute of Science. Rehovot, Israel. **April, May 2010**
Visiting Scientist with Prof. Moni Naor

Microsoft Research – New England Lab. Cambridge, MA. **Summer 2009**
Summer Research Intern with Dr. Yael Taumann Kalai

Bell Laboratories. Alcatel-Lucent. Murray Hill, NJ. **Summer 2008**
Summer Research Intern with Dr. Juan Garay

University of Århus. Århus, Denmark. **Summer 2007**
Summer Research Intern with Prof. Ivan Damgård

Industry Experience

Applied Predictive Technologies. Arlington, VA. **August, 2005 - August, 2006**

Software Engineer

Teaching	**Northeastern University.** Boston, MA USA.	
	CS 3800 Theory of Computation	Fall, 2016
	CS 7880 Graduate Cryptography	Fall, 2015
	CS 3800 Theory of Computation	Spring, 2015
	CS 3800 Theory of Computation	Fall, 2014
	CS 6750 Introduction to Cryptography	Spring, 2014
	CS 3800 Theory of Computation	Fall, 2013

Internal	**Northeastern University.** Boston, MA USA.	
Committees	PhD CS Curriculum Committee	2017
	Hiring committee	2016
	PhD committee	2015
	MS committee	2014
	PhD committee	2013